07813994 **Image available**
PRINTER, INFORMATION PROCESSOR, PRINT SERVER, CONTROL METHOD FOR PRINTER AND PRINT SYSTEM AND INFORMATION PROCESSING METHOD

PUB. NO.: 2003-308194 [JP 2003308194 A]
PUBLISHED: October 31, 2003 (20031031)
INVENTOR(s): TAKAGI YOSHIHIRO
APPLICANT(s): CANON INC
APPL. NO.: 2002-113629 [JP 2002113629]
FILED: April 16, 2002 (20020416)
INTL CLASS: G06F-003/12; B41J-005/30; G06F-015/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a secure print system in which security is improved.

SOLUTION: A print server 200 produces unique data in response to receiving of a user name 301 from a host computer 100 and transmits the data to the host computer 100 together with a job ID (302). Besides, a password corresponding to the user name is obtained from a database 400 and encrypted by using the produced unique data to produce an encrypted password, and the encrypted password is paired with the job ID and stored in a database 401. The host computer 100 encrypts the password by using the received unique data and transmits a print job embedded with the obtained encrypted password and the received job ID (303). When the job ID and the encrypted password registered in the database 401 are the same as the job ID and the encrypted password received from the host computer 100, the relevant print job is outputted to a printer 300.

?

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－308194
（Ｐ2003－308194Ａ）
(43)公開日　平成15年10月31日(2003.10.31)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ06Ｆ　3/12		Ｃ06Ｆ　3/12	Ｋ	2Ｃ187
Ｂ41Ｊ　5/30		Ｂ41Ｊ　5/30	Ｚ	5Ｂ021
Ｇ06Ｆ　15/00	330	Ｇ06Ｆ　15/00	330Ｅ	5Ｂ085

審査請求　未請求　請求項の数22　ＯＬ　（全 11 頁）

(21)出願番号　特願2002－113629(Ｐ2002－113629)

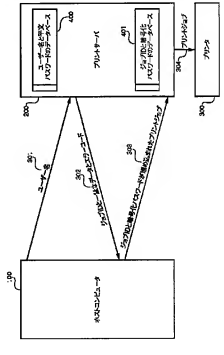
(22)出願日　平成14年4月16日(2002.4.16)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　高木　義博
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100076428
弁理士　大塚　康徳　（外３名）

Ｆターム(参考)　2Ｃ187 AD03 AD04 AD14 AE07 AE13 BF26 GD02
5Ｂ021 AA01 BB04 NN18
5Ｂ085 AE03 AE09 AE23 BA07 BG02 BC07

(54)【発明の名称】　印刷装置、情報処理装置、プリントサーバ、印刷装置及び印刷システムの制御方法並びに情報処理方法

(57)【要約】
【課題】セキュリティ性を向上したセキュアプリントシステムを提供する。
【解決手段】プリントサーバ200はホストコンピュータ100からのユーザ名301の受信に応じて一意なデータを生成し、ジョブＩＤとともにホストコンピュータ100に送信する（302）。また、このユーザ名に対応するパスワードをデータベース400から得て、生成した一意なデータを用いて暗号化して暗号化パスワードを生成し、ジョブＩＤと対にしてデータベース401に格納する。ホストコンピュータ100は、受信した一意なデータを用いてパスワードを暗号化し、得られた暗号化パスワードと受信したジョブＩＤを埋め込んだプリントジョブを送信する（303）。データベース401に登録されたジョブＩＤと暗号化パスワードが、ホストコンピュータ100より受信したジョブＩＤと暗号化パスワードと同一である場合には、当該プリントジョブをプリンタ300に出力する。



【特許請求の範囲】

【請求項１】　ユーザ名の受信に応じて一意なデータを生成する生成手段と、
前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋めこまれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、
前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブによる印刷を実行させる印刷制御手段とを備えることを特徴とする印刷装置。

【請求項２】　ユーザ名とパスワードを対にして記憶する第１記憶手段を更に備え、
前記暗号化手段は、前記ユーザ名に対応するパスワードを前記第１記憶手段より取得することを特徴とする請求項１に記載の印刷装置。

【請求項３】　受信したユーザ名が前記第１記憶手段に記憶されていない場合に、該ユーザ名の送信元に対してエラーを通知する通知手段を更に備えることを特徴とする請求項１に記載の印刷装置。

【請求項４】　前記生成手段は、前記一意なデータとともにジョブＩＤを生成し、
前記送信手段は、前記一意なデータとともに前記ジョブＩＤを前記送信元に送信し、
前記暗号化手段は、前記暗号化パスワードと前記ジョブＩＤを対にして第２記憶手段に記憶し、
前記比較手段は、前記プリントジョブに埋めこまれた暗号化パスワードとジョブＩＤの対を、前記第２記憶手段に記憶されている暗号化パスワードとジョブＩＤの対と比較することを特徴とする請求項１に記載の印刷装置。

【請求項５】　前記印刷制御手段は、前記プリントジョブによる印刷を実行した場合に、前記第２記憶手段に記憶された、当該プリントジョブに対応する暗号化パスワードとジョブＩＤを消去することを特徴とする請求項４に記載の印刷装置。

【請求項６】　プリントジョブの送信に先立ってユーザ名を送信する第１送信手段と、
前記第１送信手段による送信に応じて受信された一意的なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、
前記暗号化パスワードをプリントジョブに埋め込む埋め込み手段と前記暗号化パスワードの埋め込まれたプリントジョブを送信する第２送信手段とを備えることを特徴とする情報処理装置。

【請求項７】　ユーザ名とパスワードの入力を促すインターフェースを提供することを特徴とする請求項６に記載の情報処理装置。

【請求項８】　前記埋め込み手段は、前記暗号化パスワードと、前記第１送信手段による送信に応じて前記一意的なデータとともに受信されたジョブＩＤとを前記プリントジョブに埋め込むことを特徴とする請求項６に記載の情報処理装置。

【請求項９】　ユーザ名の受信に応じて一意なデータを生成する生成手段と、
前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋めこまれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、
前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブを外部の印刷装置にたいして出力する出力手段とを備えることを特徴とするプリントサーバ。

【請求項１０】　ユーザ名とパスワードを対にして記憶する第１記憶手段を更に備え、
前記暗号化手段は、前記ユーザ名に対応するパスワードを前記第１記憶手段より取得することを特徴とする請求項９に記載のプリントサーバ。

【請求項１１】　受信したユーザ名が前記第１記憶手段に記憶されていない場合に、該ユーザ名の送信元に対してエラーを通知する通知手段を更に備えることを特徴とする請求項９に記載のプリントサーバ。

【請求項１２】　前記生成手段は、前記一意なデータとともにジョブＩＤを生成し、
前記送信手段は、前記一意なデータとともに前記ジョブＩＤを前記送信元に送信し、
前記暗号化手段は、前記暗号化パスワードと前記ジョブＩＤを対にして第２記憶手段に記憶し、
前記比較手段は、前記プリントジョブに埋めこまれた暗号化パスワードとジョブＩＤの対を、前記第２記憶手段に記憶されている暗号化パスワードとジョブＩＤの対と比較することを特徴とする請求項９に記載のプリントサーバ。

【請求項１３】　前記出力手段は、前記プリントジョブによる印刷を実行した場合に、前記第２記憶手段に記憶された、当該プリントジョブに対応する暗号化パスワードとジョブＩＤを消去することを特徴とする請求項１２に記載のプリントサーバ。

【請求項１４】　プリントジョブを発行する第１装置と該プリントジョブを処理する第２装置とを含むシステムであって、

前記第１装置よりプリントジョブの送信に先立ってユーザ名を送信する第１送信手段と、
前記第２装置において前記ユーザ名の受信に応じて一意なデータを生成し、第１装置に送信する第２送信手段と、
前記第１及び第２装置のそれぞれにおいて、前記一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、
前記暗号化パスワードの埋め込まれたプリントジョブを前記第２装置へ送信する第３送信手段と、
前記プリントジョブに埋め込まれた暗号化パスワードと、前記第２装置の前記暗号化手段によって得られた暗号化パスワードを比較する比較手段と、
前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブを出力する出力手段とを備えることを特徴とする印刷システム。
【請求項１５】　前記第２装置は外部に印刷装置を接続するプリントサーバであることを特徴とする請求項１４に記載の印刷システム。
【請求項１６】　前記第２装置は印刷装置であることを特徴とする請求項１４に記載の印刷システム。
【請求項１７】　ユーザ名の受信に応じて一意なデータを生成する生成工程と、
前記生成工程で生成された一意なデータを前記ユーザ名の送信元に送信する送信工程と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化工程と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋めこまれた暗号化パスワードを抽出し、前記暗号化工程で生成した暗号化パスワードと比較する比較工程と、
前記比較工程により両暗号化パスワードが一致した場合、前記プリントジョブによる印刷を実行させる印刷制御工程とを備えることを特徴とする印刷装置の制御方法。
【請求項１８】　プリントジョブの送信に先立ってユーザ名を送信する第１送信工程と、
前記第１送信工程による送信に応じて受信された一意的なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化工程と、
前記暗号化パスワードをプリントジョブに埋め込む埋め込み工程と前記暗号化パスワードの埋め込まれたプリントジョブを送信する第２送信工程とを備えることを特徴とする情報処理方法。
【請求項１９】　ユーザ名の受信に応じて一意なデータを生成する生成工程と、
前記生成工程で生成された一意なデータを前記ユーザ名の送信元に送信する送信工程と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化工程と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋めこまれた暗号化パスワードを抽出し、前記暗号化工程で生成した暗号化パスワードと比較する比較工程と、
前記比較工程により両暗号化パスワードが一致した場合、前記プリントジョブを外部の印刷装置にたいして出力する出力工程とを備えることを特徴とする情報処理方法。
【請求項２０】　プリントジョブを発行する第１装置と該プリントジョブを処理する第２装置とを含むシステムの制御方法であって、
前記第１装置よりプリントジョブの送信に先立ってユーザ名を送信する第１送信工程と、
前記第２装置において前記ユーザ名の受信に応じて一意なデータを生成し、第１装置に送信する第２送信工程と、
前記第１及び第２装置のそれぞれにおいて、前記一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化工程と、
前記暗号化パスワードの埋め込まれたプリントジョブを前記第２装置へ送信する第３送信工程と、
前記プリントジョブに埋め込まれた暗号化パスワードと、前記第２装置の前記暗号化工程によって得られた暗号化パスワードを比較する比較工程と、
前記比較工程により両暗号化パスワードが一致した場合、前記プリントジョブを出力する出力工程とを備えることを特徴とする印刷システムの制御方法。
【請求項２１】　請求項１８又は１９のいずれかに記載の情報処理方法をコンピュータによって実現するための制御プログラム。
【請求項２２】　請求項１８又は１９のいずれかに記載の情報処理方法をコンピュータによって実現するための制御プログラムを格納した記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク等を介して複数のユーザが共有して使用する印刷システムに関し、さらに詳しくはいわゆるセキュアプリント機能を有する印刷システムに関するものである。
【０００２】
【従来の技術】ネットワーク等を介して複数のユーザが共用して使用するプリンタ装置においては、ユーザ認証による印刷実行の制限を実現する、所謂セキュアプリントを実現するものがある。このセキュアプリントは、一般的には、プリントジョブにユーザ名と平文パスワードもしくは可逆暗号化パスワードを埋め込むことによって実現されている。

【０００３】
【発明が解決しようとする課題】そのため次のような問題が発生する。
１．アリントジョブをファイル化して、アリントジョブを解析することでパスワードが簡単に漏洩してしまう。
２．ファイル化したアリントジョブをプリンタへ繰り返し送信することによって、何度でも印刷出来てしまう。
【０００４】更に、ネットワーク等を介して複数のユーザが共用して使用するアリンタ装置において、アリンタ装置自体にユーザ認証の機能が無い場合は、セキュアアリントそのものが行えないことが多い。
【０００５】本発明は上記課題に鑑みなされたもので、その目的は、セキュリティ性を向上したセキュアアリントシステムを提供可能とすることにある。また、本発明の他の目的は、ファイル化されたアリントジョブを解析してもパスワードの判別を不可能として、セキュリティを向上することにある。また、本発明の他の目的は、アリントジョブが１回しか実行されないようにして、セキュリティの向上を図ることにある。更に、本発明の他の目的は、ユーザ認証機能を持たないアリンタ装置であってもセキュアアリントを実現可能とすることにある。
【０００６】
【課題を解決するための手段】上記の目的を達成するための本発明による印刷装置は以下の構成を備える。すなわち、ユーザ名の受信に応じて一意なデータを生成する生成手段と、前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、前記一意なデータの送信に応じて受信されたアリントジョブに埋め込まれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、前記比較手段により両暗号化パスワードが一致した場合、前記アリントジョブによる印刷を実行させる印刷制御手段とを備える。
【０００７】また、上記の目的を達成するための本発明による情報処理装置は、アリントジョブの送信に先立ってユーザ名を送信する第１送信手段と、前記第１送信手段による送信に応じて受信された一意的なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、前記暗号化パスワードをアリントジョブに埋め込む埋め込み手段と前記暗号化パスワードの埋め込まれたアリントジョブを送信する第２送信手段とを備える。
【０００８】また、上記の目的を達成するための本発明の他の態様によれば、以下の構成を備えるアリントサーバが提供される。すなわち、ユーザ名の受信に応じて一意なデータを生成する生成手段と、前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、前記一意なデータの送信に応じて受信されたアリントジョブに埋め込まれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、前記比較手段により両暗号化パスワードが一致した場合、前記アリントジョブを外部の印刷装置にたいして出力する出力手段とを備える。
【０００９】更に、上記の目的を達成するための本発明による印刷システムは、アリントジョブを発行する第１装置と該アリントジョブを処理する第２装置とを含むシステムであって、前記第１装置よりアリントジョブの送信に先立ってユーザ名を送信する第１送信手段と、前記第２装置において前記ユーザ名の受信に応じて一意なデータを生成し、第１装置に送信する第２送信手段と、前記第１及び第２装置のそれぞれにおいて、前記一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、前記暗号化パスワードの埋め込まれたアリントジョブを前記第２装置へ送信する第３送信手段と、前記アリントジョブに埋め込まれた暗号化パスワードと、前記第２装置の前記暗号化手段によって得られた暗号化パスワードを比較する比較手段と、前記比較手段により両暗号化パスワードが一致した場合、前記アリントジョブを出力する出力手段とを備える。
【００１０】また、本発明によれば、上記印刷装置、情報処理装置、印刷システムに対応する、印刷処理のための方法が提供される。また、それら方法をコンピュータによって実行させるための制御プログラムも提供される。
【００１１】
【発明の実施の形態】以下添付図面を参照して、本発明にかかる実施形態を詳細に説明する。
【００１２】＜第１実施形態＞
［システム構成］図１は第１実施形態のシステム構成例を示す図である。本実施形態によるセキュアアリント機能は、図１の各ホストコンピュータ１００とアリントサーバ２００との間で実現される。また、図２は図１のホストコンピュータ及びアリントサーバとアリンタの構成例を示すブロック図である。
【００１３】本実施形態のセキュアアリントシステムは、図１に示すように、オペレーティングシステム（以降、ＯＳと表記）による動作環境を提供するホストコンピュータ１００と、アリントサーバ２００とアリンタ３００から構成される。ホストコンピュータ１００のＯＳは、Windows（登録商標）（Microsoft社製）を想定しているがこれに限られるものではない。
【００１４】ホストコンピュータ１００は、ＣＰＵ１０４を備える。ＣＰＵ１０４は、ＲＯＭ１０５に格納されている基本入出力プログラム（ＢＩＯＳ）に従ってＯＳ（Operating system）プログラムを実行することによ

り、OSを構築するとともに、このOS上で対応するアプリケーションプログラムをRAM106を作業領域として実行して対応する処理を行う。RAM106には、上述のOSプログラム、アプリケーションプログラムおよびそれの実行に必要なデータがハードディスク装置（HD）103からロードされる。

【0015】ハードディスク装置103には、上述のOSプログラムおよび対応するアプリケーションプログラムが格納されている。なお、本実施形態では、アプリケーションプログラムを格納する記憶装置としてハードディスク装置を用いているが、このハードディスク装置に加えて他の記憶装置例えばFD（フロッピィディスク装置）、CDROM（CDROM読取装置）などを用いて対応するアプリケーションプログラムを格納するように構成してもよい。

【0016】CPU104には、上述のROM105、RAM106とともにKBC（キーボードコントローラ）107、CRTC（ディスプレイコントローラ）108、HDC（ハードディスクコントローラ）109、イーサネット（登録商標）I/F110がCPUバス111を介して接続されている。

【0017】KBC107は、キーボード、マウスなどの入力装置101から入力されたキー信号、指示信号を受け取り、CPUバス111を介してCPU104に伝送するための制御を行う。CRTC108は、CPU104によるアプリケーションの実行結果などをディスプレイ102に表示するための表示制御を行う。HDC109は、ハードディスク装置103へのデータの書込み、読出しを制御する。イーサネットI/F110はイーサネットに接続するためのインターフェースである。第1実施形態では、イーサネットとイーサネットI/F110を介してプリントサーバ200を接続し、このプリントサーバ200との間で所定の通信プロトコルを用いて通信を行う。

【0018】このハードディスク装置103に格納されているアプリケーションプログラムには、印刷制御プログラムが含まれ、これらプログラムをCPU104が読み出して実行することによって印刷制御環境が構築される。印刷制御の詳細については後述する。

【0019】プリントサーバ200の構成において、入力装置201、ディスプレイ202、HD203、CPU204、ROM205、RAM206、KBC207、CRTC208、HDC209、イーサネットI/F210及びCPUバス211の各構成は、ホストコンピュータ100で示した参照番号101～111の各構成と同様のため説明は省略する。

【0020】プリンタ300は、プリントサーバ200のイーサネットI/F210と接続され、プリントサーバ200との間で所定の通信プロトコルを用いて通信を行うためのイーサネットI/F304と、ホストプリントサーバ200からイーサネットI/F304を介して入力された指示などに従いROM302に格納されている印刷制御処理、通信制御処理などの制御プログラムを実行するCPU301とを備える。CPU301が制御プログラムを実行する際の作業領域としては、RAM303が用いられる。また、RAM303は画像展開処理のページメモリとしても用いられる。

【0021】CPU301には、上述のROM302、RAM303、イーサネットI/F304とともにバスコントローラI/F305、エンジンI/F306がCPUバス307を介して接続されている。エンジンI/F306は、機構的に画像出力を行うエンジン部308との間でデータおよび信号のやり取りを行う入出力インターフェースであり、エンジンI/F306にはエンジン部308が接続されている。

【0022】[ホストコンピュータ100とプリントサーバ200とプリンタ300との間のデータフロー]図3は、ホストコンピュータ100とプリントサーバ200とプリンタ300との間のデータフローを示す図である。なお、ホストコンピュータ100とプリントサーバ200とプリンタ300との間はイーサネットで接続された状態を示したが、ネットワークを構成するものであれば、USB、IEEE1394、無線LANなど接続形態はなんでもかまわない。

【0023】ホストコンピュータ100からプリントジョブを送信する前にまずユーザ名を含んだデータがホストコンピュータ100からプリントサーバ200へ送信される（301）。それを受けてプリントサーバ200は、エラーコードとジョブIDと一意なデータを送り返す（302）。

【0024】そして、ホストコンピュータ100は、パスワードと一意なデータとに基づいて得られた暗号化パスワードと、上記ジョブIDとを埋め込んだプリントジョブをプリントサーバ200へ送信する（303）。プリントサーバ200においては、上記ジョブIDと暗号化パスワードによる認証を行ない、認証が得られたならばプリントサーバ200はプリンタ300へプリントジョブを送信し印刷を実行する（304）。

【0025】なお、プリントサーバ200は、上記認証を実行するために、ユーザ名と平文パスワードの対で構成されるデータベース400を保持する。このデータベース400は、印刷処理とは独立して管理される。データベースの管理方法としては、ユーザ名から平分パスワードを得られればよく、既存の技術を適用できるので、本実施形態において詳細な説明は省略する。また、プリントサーバ200は、一対のジョブIDと暗号化パスワードから構成されるデータベース401を保持する。このデータベース401の要素データは、印刷処理の実行毎に生成・破棄される。上記認証においては、ホストコンピュータより受信したプリントジョブに埋めこまれて

いるジョブＩＤ及び暗号化パスワードと、データベース４０１に格納されているジョブＩＤと暗号化パスワードとの比較が行われることになる。

【００２６】以上説明した処理をホストコンピュータ１００側から説明したフローチャートが図４であり、またプリントサーバ２００側から説明したフローチャートが図５である。以降、図４、図５を用いて処理の詳細を説明する。

【００２７】［ホストコンピュータ１００の処理フロー］ホストコンピュータ１００内部の処理を図４に示すフローチャートに従い説明する。

【００２８】図４で説明される全ての処理は、ホストコンピュータ１００内部で動作するプログラムによって実行される。なお、本実施形態のプログラムの実行形態は、アプリケーション、プリントスプーラ、プリンタドライバ、ランダージモニタ（処理場プリンタドライバより後段、ポートモニタより前段に位置し、双方向通信を司るモジュールで、デバイスのステータスを取得するのを主要な役割とする）など、様々な形態で実行が可能である。

【００２９】印刷処理に先立ち、まずユーザにユーザ名と平文パスワードの入力を促すダイアログボックスを表示し、ユーザ名と平文パスワードを入力させ、これらを得る（ステップＳ４０１）。そして、ユーザ名を含んだデータをプリントサーバ２００へ送信する（ステップＳ４０２）。これはユーザ名のチェックと、ジョブＩＤ及び一意なデータの送信要求を意味する。

【００３０】ステップＳ４０２で送信したユーザ名に対してプリントサーバ２００からエラーコードとジョブＩＤと一意なデータを受信する（ステップＳ４０３）。そして、エラーコードによってユーザ名が不正であったかどうかを判定する。なお、ユーザ名が不正な場合は、エラーコードのみが送信されればよく、ジョブＩＤと一意なデータは送信不要である。

【００３１】ジョブＩＤはホストコンピュータ１００で識別可能なデータ形式であればどのような形態であってもかまわない。一般にジョブＩＤは数値もしくは文字列であることが多い。一意なデータもホストコンピュータ１００で識別可能なデータ形式であればどのような形態であってもかまわない。一般に、一意なデータはタイムスタンプから生成される数値や文字列、もしくは、時刻やネットワークカードのＭＡＣアドレス（Media Access Control Address）から生成されるＧＵＩＤ（Global Unique ID）などがある。

【００３２】エラーコードが不正と判定された場合、即ち不正なユーザであると判定した場合（ステップＳ４０４）、不正なユーザである旨の通知を印刷実行者に知らせる（ステップＳ４０８）。この通知は、一般にダイアログボックス等を表示することが多い。

【００３３】正しいユーザであると判定された場合は、ステップＳ４０１で入手した平文パスワードとステップＳ４０３で入手した一意なデータを組み合わせて、これに非可逆の暗号化を施し、暗号化パスワードを得る（ステップＳ４０５）。一意なデータを組み合わせることにより印刷実行毎に暗号化パスワードを変化させることができる。なお、非可逆の暗号化処理としては、一般にＭＤ５（Message Digest 5）といったダイジェストアルゴリズムを利用したものが挙げられる。

【００３４】続いて、プリントジョブにステップＳ４０１で入手したジョブＩＤとステップＳ４０５で生成した暗号化パスワードをプリントジョブに埋め込む（ステップＳ４０６）。こうして暗号化パスワードが埋めこまれたプリントジョブをプリントサーバ２００へ送信する（ステップＳ４０７）。

【００３５】［プリントサーバ２００の処理フロー］次に、図３に示したプリントサーバ２００内部の処理を図５に示すフローチャートに従い説明する。なお、図５で説明される全ての処理は、プリントサーバ２００内部において動作するプログラムによって実行される。

【００３６】印刷処理に先立ち、まずホストコンピュータ１００からユーザ名が送信されてくる（ステップＳ５０１）。受信したユーザ名とデータベース４００に登録されているユーザ名を比較することによって、不正なユーザ名かどうかの判定を行う（ステップＳ５０２）。不正なユーザ名であると判定されたら、不正なユーザを意味するエラーコードをホストコンピュータ１００へ送信して処理を終了する（ステップＳ５１２）。

【００３７】一方、不正なユーザ名でなければ、ジョブＩＤと一意な任意のデータを生成する（ステップＳ５０３）。上述したように、ジョブＩＤはホストコンピュータ１００で識別可能なデータ形式であればどのような形態であってもかまわない。一般にジョブＩＤは数値もしくは文字列であることが多い。一意なデータもホストコンピュータで識別可能なデータ形式であればどのような形態であってもかまわない。一般に、一意なデータはタイムスタンプから生成される数値や文字列、もしくは、時刻やネットワークカードのＭＡＣアドレス（Media Access Control Address）から生成されるＧＵＩＤ（Global Unique ID）などがある。

【００３８】データベース４００に登録されていてかつステップＳ５０１で受信したユーザ名に対応した平文パスワードと、ステップＳ５０３で生成した一意なデータとを組み合わせて、非可逆の暗号化を施し、暗号化パスワードを生成する（ステップＳ５０４）。一意なデータを組みわせることにより印刷実行毎に暗号化パスワードを変化させることができる。なお、この非可逆の暗号化処理は、ホストコンピュータ１００において用いられる非可逆暗号化処理（ステップＳ４０５）と完全に同じアルゴリズムでなければならない。

【００３９】次に、ステップＳ５０３で生成したジョブ

ＩＤとステップＳ５０４で生成した暗号化パスワードとを関連付けてデータベース４０１に保存する（ステップＳ５０５）。この保存により任意のジョブＩＤから関連付けられた暗号化パスワードが取得可能になる。

【００４０】ステップＳ５０１において受信したユーザ名に対する応答として、ステップＳ５０３で生成したジョブＩＤ及び一意なデータと、成功を意味するエラーコードとをホストコンピュータ１００に送信する（ステップＳ５０６）。ステップＳ５０６によるデータの送信を受けて、ホストコンピュータは図４で説明したようにジョブＩＤと暗号化パスワードが埋めこまれたプリントジョブを出力する。よって、プリントサーバ２００は、ホストコンピュータ１００からこのプリントジョブを受信する（ステップＳ５０７）。

【００４１】このプリントジョブにはジョブＩＤと暗号化パスワードが埋め込まれているので、これらを取り出し（ステップＳ５０８）、ステップＳ５０５においてデータベース４０１に保存しておいた当該ジョブＩＤ及び暗号化パスワードと比較する（ステップＳ５０９）。

【００４２】比較の結果、完全に一致した場合は、プリントジョブをプリンタ３００へ送信して印刷を実行し（ステップＳ５１０）、ステップＳ５１１においてデータベース４０１に保存しておいた当該ジョブＩＤと暗号化パスワードを削除する（ステップＳ５１１）。このジョブＩＤと暗号化パスワードの削除により同じプリントジョブを複数回印刷することを妨げることが可能となる。

【００４３】以上説明したように第１実施形態によれば、セキュアプリント機能を持たないプリンタ装置であってもセキュアプリントシステムが実現され、さらに、ファイル化されたプリントジョブを解析してもパスワードは判別不可能であり、かつプリントジョブの印刷は１回のみ実行可能となる。

【００４４】＜第２実施形態＞第１実施形態ではプリントサーバ２００を介してプリンタ３００と接続することにより、セキュアプリントの機能を有していないプリンタであっても、セキュアプリントを実行することを可能としている。しかしながら、プリントサーバ２００のセキュアプリント機能をプリンタ自身が有する場合には、プリントサーバを介さずにセキュアプリントを実現できる。第２実施形態ではこのようなプリンタについて説明する。

【００４５】図６は第２実施形態によるプリンタシステムの構成を示す図である。プリンタ５００は共有プリンタとして、プリントサーバを介さずにネットワークに直接に接続されている。

【００４６】図７は図６のホストコンピュータとプリンタの構成例を示すブロック図である。ホストコンピュータ１００の構成は図２で説明したとおりであるが、第２実施形態では、イーサネットとイーサネットＩ／Ｆ１１０を介してプリンタ５００と接続し、プリンタ５００との間で所定の通信プロトコルを用いて通信を行なう。

【００４７】プリンタ５００において、イーサネットＩ／Ｆ５０４は、ホストコンピュータ１００のイーサネットＩ／Ｆ１１０と接続され、ホストコンピュータ１００との間で所定の通信プロトコルを用いて通信を行う。ＣＰＵ５０１は、ホストコンピュータ１００からイーサネットＩ／Ｆ５０４を介して入力された指示などに従いＲＯＭ３０２に格納されている印刷制御処理、通信制御処理などの制御プログラムを実行する。

【００４８】図８は、第２の実施形態によるホストコンピュータ１００とプリンタ５００との間のデータフローを示す図である。なお、ホストコンピュータ１００とプリンタ３００との間はイーサネットで接続された状態を示したが、ネットワークを構成するものであれば、ＵＳＢ、ＩＥＥＥ１３９４、無線ＬＡＮなど接続形態はなんであってもかまわない。

【００４９】ホストコンピュータ１００からプリンタ５００へプリントジョブを送信する前にまずユーザ名を含んだデータがホストコンピュータ１００からプリンタ５００へ送信される（８０１）。それを受けてプリンタ５００は、エラーコードとジョブＩＤと一意なデータを送り返す（８０２）。

【００５０】そして、ホストコンピュータ１００は、パスワードと一意なデータとに基づいて得られた暗号化パスワードと、上記ジョブＩＤとを埋め込んだプリントジョブを生成し、プリンタ５００へ送信する（８０３）。プリンタ５００においては、上記ジョブＩＤと暗号化パスワードによる認証を行ない、認証が得られたならば当該プリントジョブに対する印刷を実行する。

【００５１】なお、第１実施形態で説明したデータベース４００、４０１は、プリンタ５００が所有することになる。そして、プリンタ５００は、第１実施形態でプリントサーバ２００が実行した図５の処理を実行することにより、セキュアプリントを実現するのである。なお、第１実施形態では、図４に示されるホストコンピュータ１００の処理はプリントサーバ２００に対するものであったが、第２実施形態では、プリンタ５００に対する処理となる。

【００５２】以上のように第２実施形態によれば、プリントサーバが不要となり、システムの簡易化を達成できる。

【００５３】＜他の実施形態＞なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【００５４】また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるい

は装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（OS）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５５】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５６】

【発明の効果】以上説明したように、本発明によれば、セキュリティ性を向上したセキュアプリントシステムが提供される。

【図面の簡単な説明】

【図１】第１実施形態のシステム構成例を示す図である。

【図２】図１のホストコンピュータ及びプリントサーバとプリンタの構成例を示すブロック図である。

【図３】ホストコンピュータ１００とプリントサーバ２００とプリンタ３００との間のデータフローを示す図である。

【図４】実施形態によるホストコンピュータの処理を説明するフローチャートである。

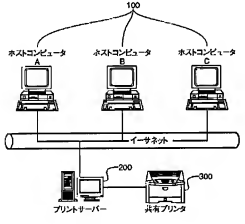
【図５】実施形態によるプリントサーバの処理を説明するフローチャートである。

【図６】第２実施形態によるプリンタシステムの構成を示す図である。

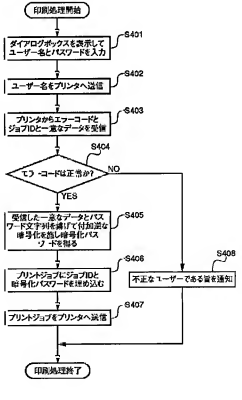
【図７】図６のホストコンピュータとプリンタの構成例を示すブロック図である。

【図８】ホストコンピュータ１００とプリンタ５００との間のデータフローを示す図である。

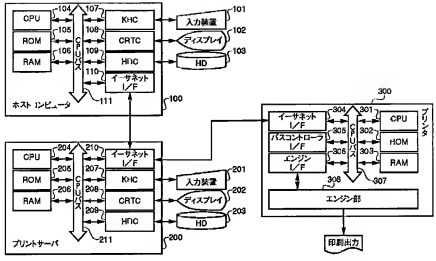
【図１】



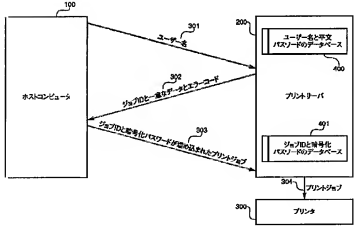
【図４】



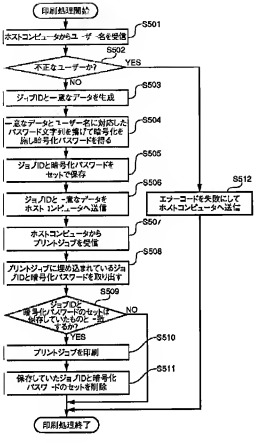
【図2】


CPU
ROM
RAM
104
105
106
107
108
109
110
111
KHC
CRTC
HFIC
イーサネットI/F
入力装置
ディスプレイ
HD
101
102
103
100
ホストコンピュータ
300
イーサネットI/F
バスコントローラI/F
エンジンI/F
304
305
306
301
302
303
CPU
ROM
RAM
307
308
エンジン部
プリンタ
印刷出力
204
205
206
210
207
208
209
211
200
201
202
203
プリントサーバ

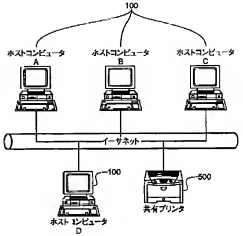
【図3】


100
ホストコンピュータ
301
ユーザー名
302
ジョブIDと一致するデータビューコード
303
ジョブIDと紐付けパスワードが組み込まれたプリントジョブ
200
ユーザー名と平文パスワードのデータベース
400
プリントサーバ
401
ジョブIDと紐付け暗号化パスワードのデータベース
304
プリントジョブ
300
プリンタ

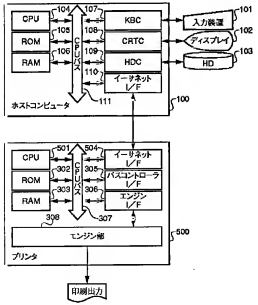
【図5】


印刷処理開始
S501
ホストコンピュータからユーザー名を受信
S502
不正なユーザーか?
YES
NO
S503
ジョブIDと一意なデータを生成
S504
一意なデータとユーザー名に対応したパスワード文字列を鍵にて暗号化を施し暗号化パスワードを得る
S505
ジョブIDと暗号化パスワードをセットで保存
S506
ジョブIDと一意なデータをホストコンピュータへ送信
S512
エラーコードを失敗にしてホストコンピュータへ送信
S507
ホストコンピュータからプリントジョブを受信
S508
プリントジョブに埋め込まれているジョブIDと暗号化パスワードを取り出す
S509
ジョブIDと暗号化パスワードのセットは保存しているものと一致するか?
NO
YES
S510
プリントジョブを印刷
S511
保存していたジョブIDと暗号化パスワードのセットを削除
印刷処理終了

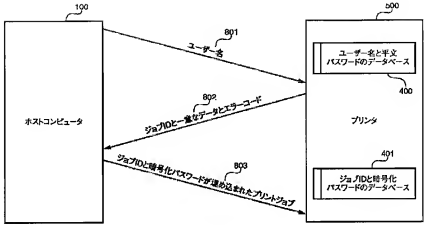
【図6】


100
ホストコンピュータ A
ホストコンピュータ B
ホストコンピュータ C
イーサネット
100
ホストコンピュータ D
500
共有プリンタ

【図7】


CPU
ROM
RAM
104
105
106
107
108
109
110
111
KBC
CRTC
HDC
イーサネットI/F
BUS
入力装置
ディスプレイ
HD
101
102
103
ホストコンピュータ
100
501
502
503
504
505
506
507
308
イーサネットI/F
パスコントローラI/F
エンジンI/F
エンジン部
500
プリンタ
印刷出力

【図8】


100
ホストコンピュータ
500
プリンタ
801
ユーザー名
802
ジョブIDと一意なデータとエラーコード
803
ジョブIDと暗号化パスワードが埋め込まれたプリントジョブ
ユーザー名と平文パスワードのデータベース
400
401
ジョブIDと暗号化パスワードのデータベース